

ZENworks 11 SP3

Test Scenarios for *Endpoint Security Management*

This document contains test scenarios for ZENworks 11 SP3 Beta.

Purpose of the Test Scenarios

The purpose of these exercises is to help you get familiar with some of the new features included in ZENworks 11 SP3 Endpoint Security Management.

Assumption

- You have installed ZENworks 11 SP3. For instructions, see the *ZENworks 11 SP3 Installation Guide* (<http://www.novell.com/documentation/zenworks113/>).

Test Scenarios

1. [Apply a Data Encryption Policy that Requires a One-Time Entry of the Encryption Password for Removable Storage Devices](#)
2. [Audit Changes to Endpoint Security Policies](#)
3. [Audit File Copies from a Device to Removable Storage](#)

Test Scenario #1: Apply a Data Encryption Policy that Requires a One-Time Entry of the Encryption Password for Removable Storage Devices

Objective

This scenario will enable you to provide an encryption password for removable storage device encryption one time only.

In previous releases, a user was required to provide a encryption password for removable storage devices each time a new session started (for example, each time the device restarted). You can now configure the Data Encryption policy to enable a one-time entry of the encryption password and have it persisted across sessions.

Procedure

1. In ZENworks Control Center, click *Policies*.
2. In the Policies panel, click *New > Policy*.
3. For the policy platform, select *Windows*, then click *Next*.
4. For the policy category, select *Windows Endpoint Security Policies*, then click *Next*.
5. Select *Data Encryption Policy* as the policy type, then click *Next*.
6. On the Define Details page, specify a policy name, then click *Next*.
7. On the Configure Data Encryption Settings page:
 - a) Select *Enable encryption for removable storage devices*.
 - b) Select *Enable encryption via user-defined password*.
 - c) Leave the *Apply password encryption to entire device* option selected.
 - d) Select the *Prompt user for encryption password one time only* option.
 - e) Click *Next*.
8. Review the policy details in the Summary page, then click *Finish* to create the policy.
9. Assign the policy to a device.
10. On the device, refresh the ZENworks Adaptive Agent to apply the policy.
11. Insert a removable storage device (for example, a USB drive).
12. When prompted to encrypt the drive, click *Continue*.

13. Copy a file to the removable storage device. When prompted to enter an encryption password, do so.
14. Reboot the device.
15. Copy another file to the removable storage device. You are not prompted to enter an encryption password. The previously entered password is used for encrypting the file.

Expected Results

After successful enforcement of the policy on the endpoint device, you are prompted one time to supply a password for encrypting files copied to a removable storage devices. The password is persisted across sessions.

Test Scenario #2: Audit Changes to Endpoint Security Policies

Objective

To turn on auditing of security policies so that changes to the policies are recorded.

Prerequisites

- At least one existing Endpoint Security policy. For help in creating an Endpoint Security policy, see the *ZENworks 11 SP3 Endpoint Security Policies Reference*. (<http://www.novell.com/documentation/zenworks113/>).

Procedure

Complete the steps in the following sections to enable the audit change event, make changes to a security policy, and view the generated audit change event.

Enable the Audit Change Event for Security Policies

1. In the left navigation pane of ZENworks Control Center, click *Configuration*.
2. In the *Configuration* tab, under *Management Zone Settings*, click *Audit Management*.
3. Click *Events Configuration*.
4. Under *Change Events*, click *Add* to display the *Add Change Events* dialog box.
5. Expand the Change Events tree and select *Endpoint Security Policy Modified*.
6. In the *Event Settings* section, set the *Event Classification* to *Informational*.
7. Specify the *Days to Keep* as 30.
8. Click *OK* to add the event and close the *Add Change Events* dialog box.

Modify a Security Policy Setting

1. In the left navigation pane of ZENworks Control Center, click *Policies*.
2. In the Policies list, double-click a security policy to display its properties.
3. Click *Details* to display the policy's settings.
4. Change one of the settings, then click *Apply* to save the changes.

View the Change Event

1. In the left navigation pane of ZENworks Control Center, click *Dashboard*.

2. In the *Top 5 Change Events by Administrator* section, click *Endpoint Security Policy Modified*.

If *Endpoint Security Policy Modified* is not in the list, wait a few minutes and click the Refresh icon in the menu bar.

3. Click the Endpoint Security Policy Modified event in the list to display its details.

Expected Results

- The change event is displayed in the Dashboard.

Test Scenario #3: Audit File Copies from a Device to Removable Storage

Objective

To turn on Endpoint Security auditing that enables the monitoring and recording of files copied from a device to removable storage connected to that device.

Prerequisites

- Completion of [Test Scenario #1: Apply a Data Encryption Policy that Requires a One-Time Entry of the Encryption Password for Removable Storage Devices](#) so that a Data Encryption policy with removable storage device encryption is applied to a Windows device.

Procedure

Complete the steps in the following sections to enable the agent change event, copy files to the removable storage device, and view the generated agent event in ZENworks Control Center.

Enable the Audit Agent Events for Endpoint Security

1. In the left navigation pane of ZENworks Control Center, click *Configuration*.
2. In the *Configuration* tab, under *Management Zone Settings*, click *Audit Management*.
3. Click *Events Configuration*.
4. Under *Agent Events*, click *Add* to display the *Add Agent Events* dialog box.
5. Expand the ZENworks Endpoint Security section of the Agent Events tree.
6. Select the *Count of Files Copied to Removable Storage Device* event and the *File Activity* event.
7. In the *Event Settings* section, set the *Event Classification* as *Informational*.
8. Specify the *Days to Keep* as 30.
9. Leave the *Sample Frequency* set to 10 minutes.
10. Click *OK* to add the event and close the *Add Change Events* dialog box.

Copy Files to a Windows Device's Removable Storage Device

1. At the Windows device where you have applied the Data Encryption policy required by the prerequisites, insert a removable storage device (for example, a USB drive).
2. If prompted to encrypt the drive, click *Continue*.
3. Copy one or more files to the removable storage device. If prompted to enter an encryption password, do so.

View the Agent Event

1. Wait 30 minutes after the file copy on the device.
2. In the left navigation pane of ZENworks Control Center, click *Dashboard*.
3. Click *Count Of Files Copied To Removable Storage Device*.

If *Count Of Files Copied To Removable Storage Device* is not in the list, wait a few minutes and click the Refresh icon in the menu bar.

4. Click the *Count Of Files Copied To Removable Storage Device* event in the list to display its details.

The event lists the number of files copied to the device. The count is intended to be an indicator of file copy activity, not an absolute count. The count is incremented every time a write occurs on the removable storage device. Multiple writes can occur for a single file copy, which means that the file count can be higher than the actual number of files copied.

Expected Results:

- The agent event is displayed in the Dashboard.